DIR CYBERSECURITY INSIGHT

Newsletter

April 2014

ADDRESSING THE EVER CHANGING RISKS FOR THE STATE OF TEXAS

IN THIS ISSUE

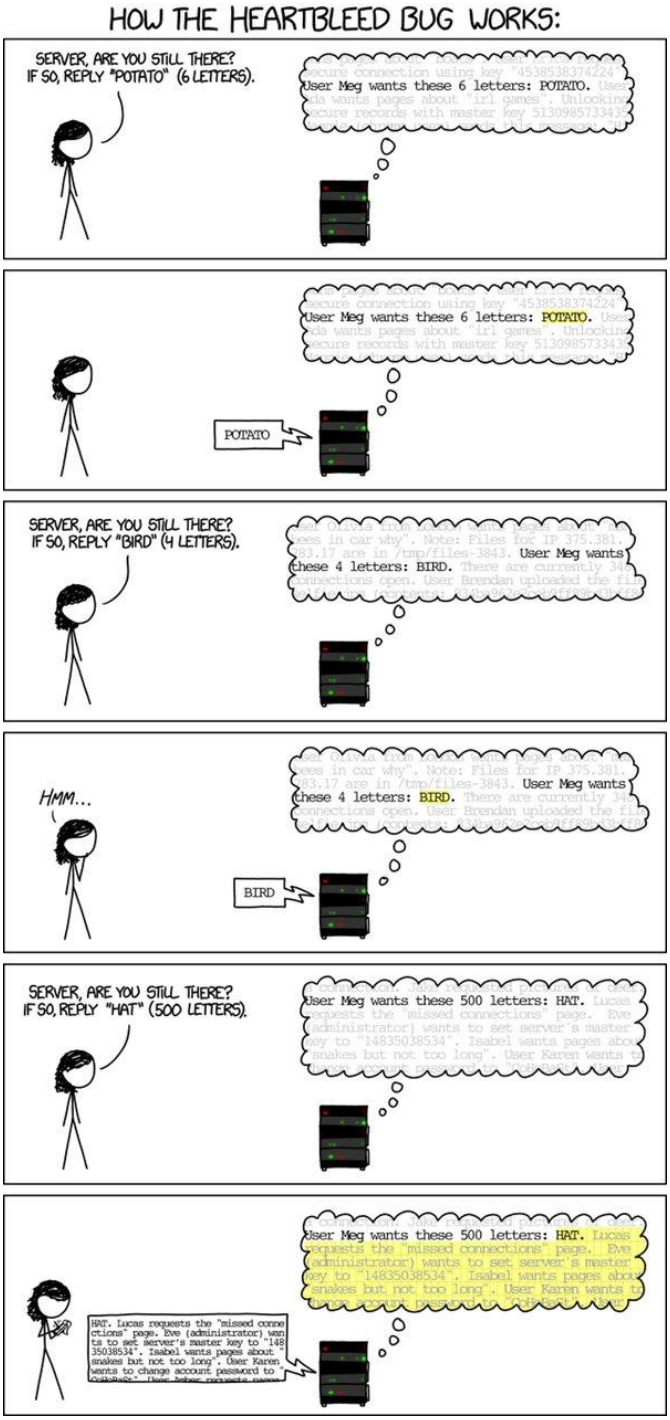
Four questions for your CIO

Shaping your elevator pitch for Executive Management

How often do you interact with your Executive Staff, CIO or IT Director? Here are some questions to consider to use in a relevant conversation with them:

- What is the budget devoted to information security and risk management functions of the organization, and how is it measured?
  - % of IT Spend
  - % of Company Spend
  - $ per employee
- Which personnel are devoted to information security and risk management?
  - Who?
  - How many?
  - How often do you hear from them?
- Which security functions are performed throughout the organization and how are those functions determined?
  - Need?
  - Ability?
  - Capability?
- How are you managing and measuring technology risk throughout the organization?
  - Decision process
  - Loss Expectancy
  - Acceptable Loss

The Heartbleed Bug



On Tuesday, April 8th, 2014, a vulnerability discovered in OpenSSL's implementation of the TLS 'heartbeat' extension was announced, and soon after named Heartbleed. This XKCD diagram does an excellent job describing how the Heartbleed Vulnerability works.

Six Simple Heartbleed Response Steps for IT:

1. Check for vulnerable software versions.
2. Patch vulnerable systems.
3. Install new SSL certificates.
4. Tell everyone that vulnerable systems are *fixed*.
5. Mandate admins change their passwords.
6. Recommend users change passwords.

Useful links:

http://heartbleed.com/

The Heartbleed Hit List:

http://mashable.com/2014/04/09/heartbleed-bug-websites-affected/?utm_cid=mash-com-fb-main-link

Remember to revoke and reissue certificates after vulnerable servers are patched, and then advise application users to change their passwords.

SPOTLIGHT

Mary Dickerson

Mary E. Dickerson, MBA, CISSP, CISM, PMP
Executive Director, IT Security
Chief Information Security Officer
University of Houston | University of Houston System

Tell us about yourself.

I have a BS degree from Texas A&M (yes, I am a proud Aggie) and an MBA from the University of Houston (and also a proud Cougar!). Before I made my way into IT, I was fortunate to have had many great professional experiences as a church youth minister, a high school debate coach, a paralegal, and an office manager. I am a CISSP, CISM, PMP, and MCSE (which really just means I have lots of experience taking tests. I have worked at UH for 16 years and have enjoyed watching the university change and grow. In 2011, I was honored to be appointed to serve on the Texas CyberSecurity Education and Economic Development Council established by SB 988. In what little spare time I have (sleep is highly overrated) I enjoy serving as a volunteer firefighter/medic and, with my awesome husband, the adventures of raising our son.

How did you come to the security field?

I was working as an enterprise system administrator and had just completed several large-scale projects: AD design and implementation, Exchange RDP, etc., when I was assigned a new project – PCI compliance! Compliance was associated with the IT security team, instead of the IT server team and the rest is history…

Tell us how information security has changed since you started in your role.

IT security used to be seen as more of a police force – identify and stop the hackers looking to break in and do bad things. Now, IT security is more often seen as a business enabler and an important partner in an organization's overall risk strategy.

What do you like best of your job?

The People! The Challenges! I have no idea what it is to be bored – every day presents new experiences and opportunities.

Who are your users/customers, and what is one of the most challenging area for you?

There are approximately 80,000 faculty, staff and students across the University of Houston System, which is made up of 4 universities and multiple campuses. A university is very similar to a small city – while we have compliance requirements for every industry (healthcare, payment cards, law enforcement, residence halls), we also have to balance everyday customer needs in a very flexible open environment.

What other career would you have liked to pursue?

It would be fun to run an old-fashioned book or craft store. No technology allowed!

What has been the greatest challenge that you have faced, and how did you resolved it?

In 2012, I was unexpectedly hospitalized for 29 days – 14 days spent in ICU on a ventilator. After I was released from the hospital I had to learn how to walk again and had to rely on family and friends for help with daily activities. However, through the phenomenal support and encouragement of family, friends, and colleagues, I not only am walking again, but have done 5 – 5K runs since 2012. ☺

Tell us about your most proud accomplishment?

After being hospitalized and not able to walk, managing to stand up off of a couch without assistance. It sounds simple, and something we all probably take for granted – but when you have had to rely on someone else just to get up, it is monumental!

People would be surprised to know that you…

I am a Texas SFFMA-Certified Firefighter.

What is the best advice you have received and that you have used?

"The secret to having it all is believing you already do." Author unknown.

What would be your advice for a new security professional?

IT security is primarily about relationships – between people, between technologies, between information, and the people that use the information. Don't be afraid to ask questions and ask for help from other IT security professionals. Fundamentally, we are all on the same team. And most of us know at little about having fun, too!

Collaboration Opportunities

Statewide Information Security Advisory Committee

The Statewide Information Security Advisory Committee (SISAC) provides guidance to the Texas Department of Information Resources (DIR) on the Statewide Information Security Program. The committee, chartered by DIR in 2011, is comprised of information security professionals from state and local government and representatives from private industry. SISAC aims to cross-pollinate ideas and best practices among its members and make recommendations to DIR for more effective information security operations by:

- Facilitating an open forum for the sharing and discussion of cybersecurity issues and concerns
- Assisting in reviewing enterprise-wide cybersecurity products, policies, and services
- Proactively discussing current and emerging cybersecurity risks and mitigation strategies
- Forming recommendations for DIR on cybersecurity policies and practices to be implemented by state government
- Acting as a communication channel for promoting and supporting security policies and initiatives

SISAC makes use of subcommittees and work groups to conduct specific work by involving additional subject matter experts. Currently, SISAC has six subcommittees established to address key initiatives within the overall Statewide Information Security Program.

Join a Team

Contribute to SISAC by participating in one of its subcommittees. These workgroups meet on a monthly basis.

- **Communications Subcommittee**
  Communicates to the agencies the progress of the DIR Statewide Information Security Program and associated events and evaluates feedback from the agencies. To join, contact Frosty Walker, ISO, Texas Education Agency (Frosty.Walker@tea.state.tx.us).

- **Privacy Subcommittee**
  Facilitates collaboration with agency personnel responsible for privacy policy functions associated with the protection of citizen privacy and developing privacy incident response procedures. To join, contact Elizabeth Rogers, Chief Privacy Officer, Texas Comptroller of Public Accounts (Elizabeth.Rogers@cpa.state.tx.us).

- **Solutions Subcommittee**
  Evaluates solutions to common problems and shares best practices among agencies. To join, contact Claudia Escobar, Department of Information Resources (Claudia.Escobar@dir.texas.gov).

- **Risk Assessment Subcommittee**
  Defines and maintains the state's risk assessment methodology. To join, contact Shirley Erp, CISO, Health and Human Services Commission (Shirley.Erp@hhsc.state.tx.us).

- **Policy Subcommittee**
  Defines the state's security policy through the development of rules, standards, policies, and guidelines. To join, contact Edward Block, Deputy CISO, Department of Information Resources **(Edward.Block@dir.texas.gov).**

- **Security Workforce Development**
  Studies security workforce issues and advises SISAC on recommendations to enhance the state's security workforce. To join, contact Jesse Rivera, CISO, Texas Comptroller of Public Accounts (Jesse.Rivera@cpa.state.tx.us).

SISAC convenes monthly and is led by Brian Engle, Chief Information Security Officer for the State of Texas. The executive sponsor of SISAC is Karen Robinson, the state's Chief Information Officer and executive director of DIR. Call 512-475-4700 for more information.

Cybersecurity Tips by MS-ISAC MULTI-STATE Information Sharing & Analysis Center

Secure your computer

Ensure your computer is current with all available patches, fixes, and upgrades. If you do not have your operating system set to automatically update, do so now by visiting your operating system's website and following the instructions. Links are provided here for Windows users and Mac users. (In addition, note that support for Windows XP ended on April 8, 2014. The end of support for Windows XP means that Microsoft will no longer provide new security updates and will therefore become a significant security risk. It is recommended that anyone using Windows XP migrates to products that are supported, such as Windows Vista, Windows 7 or 8.)

Your computer's security software should also be up-to-date. To check status, click on the icon for the security program on your system. If an update is needed, it will be indicated here. If you don't have security software installed, you need to get it. Make sure you have anti-virus and anti-spyware software installed and a firewall enabled.

Confirm that your browsers are up-to-date. Tools such as Qualys BrowserCheck or WhatBrowser can help assess status.

Secure your accounts

You probably access numerous online accounts, including social media, banking, news sites, shopping, and others. If you've been hacked, there is a chance that important passwords have been stolen. Reset your passwords for your critical accounts first, starting with your email account, followed by financial and other critical accounts. It is important to start with email accounts, since password resets for all of your other accounts are typically sent to your email.

Use separate and unique ID/password combinations for different accounts and avoid writing them down. Make the passwords more complicated by combining letters, numbers, special characters, and by changing them on a regular basis. If you are unable to log into one of your accounts, contact the service provider or website immediately. Most online providers include an online form, an email address to contact, or a phone number to call.

Secure your mobile

Our increased reliance on smart devices–including mobile phones and tablets–for everyday activities has resulted in an increased number of hacking attempts against these devices. As we do with our personal computers, we have to ensure that the proper steps are taken to protect our information and devices. This includes installing security software, where available, and keeping all installed software up-to-date.

Around the Corner in Texas

Webinar

Gartner Webinar

MAY: "Sharing Data without Losing it" – *May 13th 2:00pm CDT*
JUNE: "Security in a DevOPs World" – *June 10th 2:00pm CDT*

For more information in Education visit DIR Security

Shred day

Free Shred Day for everyone

Saturday, May 17, 2014 - 8:00am - 1:30pm

The Austin chapter of ARMA International is sponsoring their 11th annual free SPRING Shred Day. With the increased awareness of identity theft, it's important to carefully dispose of personal records. Households can bring up to five boxes of paper records per household. All of the shredded material is recycled. Please make sure your records are paper only (no hard plastics, no plastic bags, electronic media or three-ring binders) and are not wet or moldy. Mobile shredding trucks will be provided by Balcones Resources, Cintas, and Iron Mountain.

ARMA International is a not-for-profit professional association and the authority on governing information as a strategic asset.

Monetary donations will be accepted with a portion of the proceeds going to ARMA Austin and the Capital Area Food Bank.

More info at: http://www.austintexas.gov/event/free-shred-day

Free Shred Day for State Agencies

CSI LEASING epc Secure IT Asset Recovery CSI/EPC are putting together a Hard Drive Shredding day in Austin again with their DDRV (Data Destruction Recycle Vehicle); our 26' box truck with a diesel generator and mobile shredder on the back of it.

For Agencies in the Northern part of the city: ***May 14th HHSC (Winters Building – C) 11AM-4PM***
For Agencies in the Southern part of the city: ***May 15th DIR (W.P. Clements Building – Breeze) 9AM-4PM***

When drives are shredded, they will provide a HIPAA destruction certificate for the State Agencies and a flash drive with a live recording of the shredding for compliance records.

For faster service please RSVP patrick.mann@epcusa.com

OCISO DIR Office of the CHIEF INFORMATION SECURITY OFFICER State of Texas